

IN THE UNITED STATES DISTRICT COURT FOR THE  
NORTHERN DISTRICT OF ILLINOIS

LINDABETH RIVERA, on behalf of herself  
and all others similarly situated,

Plaintiff,

v.

GOOGLE INC.,

Defendant.

Case No.: 1:16-cv-02714

Judge: Honorable Edmond E. Chang

Magistrate Michael T. Mason

JOSEPH WEISS, individually and on behalf  
of all others similarly situated,

Plaintiff,

v.

GOOGLE INC.,

Defendant.

**GOOGLE INC.'S MEMORANDUM OF LAW IN SUPPORT OF ITS  
CONSOLIDATED MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED  
COMPLAINTS PURSUANT TO FED. R. CIV. P. 12(b)(6)**

**TABLE OF CONTENTS**

	<b>Page</b>
I. INTRODUCTION .....	1
II. BACKGROUND .....	2
A. Illinois' Biometric Information Privacy Act.....	2
B. Plaintiffs' Allegations .....	4
III. ARGUMENT .....	6
A. The Text, Structure, and History of BIPA Demonstrate that the Statute Does Not Cover Photographs or Information Derived from Photographs .....	6
B. Even if BIPA Covers Information Derived from Photographs, the Presumption Against Extraterritoriality Establishes that the FACs Should Be Dismissed.....	13
C. Under Plaintiffs' Interpretation, BIPA Would Violate the Dormant Commerce Clause.....	15
1. The Practical Effect of BIPA, on Plaintiffs' Reading, Is to Regulate Out-Of-State Conduct.....	15
2. This Court Should Interpret BIPA to Avoid Serious Constitutional Problems.....	18
IV. CONCLUSION.....	19

# **TABLE OF AUTHORITIES**

	Page(s)
<b>CASES</b>	
<i>Am. Civil Liberties Union v. Johnson</i> , 194 F.3d 1149 (10th Cir. 1999) .....	16, 18
<i>Am. Libraries Ass’n v. Pataki</i> , 969 F. Supp. 160 (S.D.N.Y. 1997) .....	18
<i>American Booksellers Foundation v. Dean</i> , 342 F.3d 96 (2003).....	17, 18
<i>Avery v. State Farm Mut. Auto Ins. Co.</i> , 216 Ill. 2d 100 (2005) .....	13, 14
<i>Bibb v. Navajo Freight Lines</i> , 359 U.S. 520 (1959).....	18
<i>BMW of N. Am., Inc. v. Gore</i> , 517 U.S. 559 (1996).....	17
<i>Chisom v. Roemer</i> , 501 U.S. 380 (1991).....	11
<i>Cooley v. Bd. of Wardens</i> , 53 U.S. 299 (1851).....	18
<i>Dur-Ite Co. v. Indus. Comm’n</i> , 394 Ill. 338 (1946) .....	13
<i>Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. &amp; Constr. Trades Council</i> , 485 U.S. 568 (1988).....	19
<i>Graham v. Gen. U.S. Grant Post No. 2665, V.F.W.</i> , 43 Ill. 2d 1 (1969) .....	14
<i>Great Atl. &amp; Pac. Tea Co. v. Cottrell</i> , 424 U.S. 366 (1976).....	15
<i>Guinto v. Nestorowicz</i> , No. 14 C 09940, 2015 WL 3421456 (N.D. Ill. May 28, 2015) .....	13
<i>Gulf Oil Corp. v. Copp Paving Co.</i> , 419 U.S. 186 (1974).....	11

<i>Healy v. Beer Inst., Inc.</i> , 491 U.S. 324 (1989).....	15, 17, 19
<i>Hinkle by Hinkle v. Henderson</i> , 85 F.3d 298 (7th Cir. 1996) .....	12
<i>In re Facebook Biometric Info. Privacy Litig.</i> , No. 15-cv-03747-JD, 2016 WL 2593853 (N.D. Cal. May 5, 2016).....	12, 13
<i>Klein v. Depuy, Inc.</i> , 476 F. Supp. 2d 1007 (N.D. Ind. 2007), <i>aff'd</i> , 506 F.3d 553 (7th Cir. 2007).....	12
<i>Kraft, Inc. v. Edgar</i> , 561 N.E.2d 656 (Ill. 1990) .....	9
<i>Krohe v. City of Bloomington</i> , 789 N.E.2d 1211 (Ill. 2003) .....	10
<i>Laborer’s Int’l Union of N. Am., Local 1280 v. State Labor Relations Bd.</i> , 507 N.E.2d 1200 (Ill. App. Ct. 1987) .....	11
<i>Midlock v. Apple Vacations W., Inc.</i> , 406 F.3d 453 (7th Cir. 2005) .....	12
<i>Midwest Title Loans, Inc. v. Mills</i> , 593 F.3d 660 (7th Cir. 2010) .....	18
<i>Morley-Murphy Co. v. Zenith Elecs. Corp.</i> , 142 F.3d 373 (7th Cir. 1998) .....	18, 19
<i>Nat’l Solid Wastes Mgmt. Ass’n v. Meyer</i> , 63 F.3d 652 (7th Cir. 1995) .....	16, 17, 18
<i>Norberg v. Shutterfly, Inc.</i> , No. 15-cv-5351, 2015 WL 9914203 (N.D. Ill. Dec. 29, 2015).....	12
<i>People ex. rel. Stocke</i> , 80 Ill. App. 3d 109 (5th Dist. 1979) .....	12
<i>People v. Diggins</i> , 919 N.E.2d 327 (Ill. 2009) .....	8
<i>Pippen v. NBCUniversal Media, LLC</i> , 734 F.3d 610 (7th Cir. 2013) .....	7
<i>S. Illinoisan v. Ill. Dep’t of Pub. Health</i> , 844 N.E.2d 1 (Ill. 2006) .....	7
<i>Sam Francis Found. v. Christies, Inc.</i> , 784 F.3d 1320 (9th Cir. 2015) .....	16

<i>TelTech Sys., Inc. v. McCollum</i> , No. 08-cv-61664, 2009 WL 10626585 (S.D. Fla. July 16, 2009) .....	17
--	----

<i>Wilson v. Dep't of Revenue</i> , 169 Ill. 2d 306 (1996) .....	19
---	----

## CONSTITUTION

Commerce Clause of the United States Constitution, U.S. Const. art. I, § 8, cl. 3 .....	passim
---	--------

## STATUTES

Illinois Biometric Information Privacy Act, 740 ILCS 14/1 <i>et seq.</i> .....	passim
--	--------

Illinois Consumer Fraud and Deceptive Practices Act, 216 Ill. 2d 185 (2005) .....	14
---	----

## RULES

Fed. R. Civ. P. 12(b)(6) .....	5
--------------------------------	---

## OTHER AUTHORITIES

HB 6074, S. Floor Amend. No. 1, 99th Gen. Assemb., Reg. Sess. (Ill. May 26, 2016) .....	4
--	---

IL H.R. Tran. 2008 Reg. Sess. No. 276 (May 30, 2008) .....	10, 11, 14
--	------------

SB 2400, § 10, 95th Gen. Assemb., Reg. Sess. (Ill. Feb. 14, 2008) .....	11
---	----

SB 2400, § 10, S. Floor Amend. No. 4, 95th Gen. Assemb., Reg. Sess. (Ill. Apr. 11, 2008) .....	11
---	----

Stephen Dolezalek and Josh Freed, <i>An American Kodak Moment</i> , Third Way (Apr. 17, 2014) .....	12
--	----

## **I. INTRODUCTION**

When the Illinois General Assembly enacted the Biometric Information Privacy Act (“BIPA”) eight years ago, use of biometrics in financial transactions was on the rise. At grocery stores and gas stations across Illinois, people were paying for goods and services not by entering a PIN or signing a receipt, but by swiping a finger across a biometric scanner. The General Assembly enacted BIPA to regulate the biometric data obtained through such in-person scans. But the General Assembly was careful not to go further: it expressly does not regulate photographs or any information derived from photographs.

Despite those express exclusions, Plaintiffs claim that BIPA applies to Google Photos, an online service that helps users store and organize their photographs. It does not. BIPA regulates two types of biometric data: “biometric identifiers” and “biometric information.” “Biometric identifiers” are data obtained from a person herself through in-person scans, such as at a grocery store or a gas station. “Biometric information” is information derived from such in-person scans. Here, the only things Google obtained from Google Photos users were photographs—which BIPA expressly excludes from the definition of “biometric identifier.” And although Google allegedly derived information from those photographs to make it easier for users to organize their photo albums, BIPA expressly excludes such information from the definition of “biometric information.” The text and structure of BIPA thus foreclose Plaintiffs’ claim. And if there were any doubt about the General Assembly’s intent, the legislative history resolves it: BIPA was motivated by concerns about in-person scans like those occurring across the state, not someone grouping together photographs using photo-organizing software.

Even if BIPA were construed to apply to information derived from photographs, Plaintiffs’ claim still fails. That is because there is no indication, in the text of the statute or otherwise, that the General Assembly intended BIPA to apply extraterritorially. Thus, to sustain a claim under BIPA, Plaintiffs must allege circumstances sufficient to establish that the asserted statutory violation occurred in Illinois. Plaintiffs have not done so. They suggest that what

matters is the location of where their photographs were uploaded. But BIPA does not regulate the uploading of photographs; even under Plaintiffs' reading of BIPA, a statutory violation does not occur until Google *creates* a scan of face geometry from a photograph. And Plaintiffs have not made a single allegation about where *that* happens.

Finally, even if BIPA applied to information derived from photographs, and even if its territorial reach extended to Google's conduct, Plaintiffs would face a greater obstacle still: the United States Constitution. Under the dormant Commerce Clause of the United States Constitution, U.S. Const. art. I, § 8, cl. 3, a state statute is unconstitutional if it has the practical effect of regulating conduct beyond that state. Under Plaintiffs' interpretation, BIPA would have precisely that effect, dictating what Google may do with a photograph outside of Illinois. Indeed, the difficulty of ascertaining *ex ante* whether a particular photograph would be subject to BIPA would, by itself, leave Google with no choice but to comply with the statute everywhere. Because Illinois legislators cannot decide policy for the rest of the country, adopting Plaintiffs' reading of BIPA would render the statute unconstitutional under the dormant Commerce Clause. At the very least, Plaintiffs' interpretation would raise serious constitutional doubts. That is reason enough to reject it and to construe the statute instead to apply only to in-person scans in Illinois.

Because Plaintiffs have failed to state a claim upon which relief could be granted, the Court should dismiss their First Amended Complaints with prejudice.<sup>1</sup>

## **II. BACKGROUND**

### **A. Illinois' Biometric Information Privacy Act**

In 2008, the Illinois General Assembly enacted BIPA in response to the growing use of biometrics in "financial transactions and security screenings." 740 ILCS 14/5(a). More and more people were using "biologically unique" identifiers to "access finances or other sensitive

---

<sup>1</sup> Pursuant to the parties' stipulation of June 1, 2016 (Rivera Dkt. 44), this consolidated Motion to Dismiss seeks dismissal of both the First Amended Complaint filed by Lindabeth Rivera on May 27, 2016 (the "Rivera FAC," Rivera Dkt. 40) and the First Amended Complaint filed by Joseph Weiss on May 27, 2016 (the "Weiss FAC," Rivera Dkt. 41) (together, the "FACs").

information.” *Id.* 14/5(c). “[F]inger-scan technologies,” for example, could be found “at grocery stores, gas stations, and school cafeterias” throughout the state. *Id.* 14/5(b). And so the General Assembly enacted BIPA to address the “heightened risk for identity theft” associated with such “biometric-facilitated transactions.” *Id.* 14/5(c).

To that end, BIPA regulates “[b]iometric identifier[s]” and “[b]iometric information.” *Id.* 14/10. The statute defines “biometric identifier” to “mean[]” six specific things: “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” *Id.* These are all things derived from a person’s “biologically unique” features. *Id.* 14/5(c). Expressly excluded from the definition of “biometric identifier,” however, is a list of other things derived in person, such as “writing samples, written signatures, photographs, [and] human biological samples used for valid scientific testing or screening.” *Id.* 14/10.

“Biometric information” is defined to mean “any information, regardless of how it is captured, converted, stored, or shared, *based on* an individual’s biometric identifier used to identify an individual.” *Id.* (emphasis added). The statute expressly provides that “[b]iometric information does *not* include information derived from items or procedures excluded under the definition of biometric identifiers.” *Id.* (emphasis added).

Among other things, BIPA provides that a “private entity” may not “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, unless it first” obtains the subject’s written release. *Id.* 14/15.<sup>2</sup> BIPA also requires a “private entity in possession of biometric identifiers or biometric information [to] develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.” *Id.* BIPA grants a private right of action to “[a]ny person aggrieved by a violation of [the statute].” *Id.* 14/20.<sup>3</sup>

---

<sup>2</sup> “Written Release” is defined in the statute as “informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.” 740 ILCS 14/10.

<sup>3</sup> On May 26, 2016, the original sponsor of BIPA filed a proposed amendment to the statute. *See* HB 6074, S. Floor Amend. No. 1, 99th Gen. Assemb., Reg. Sess. (Ill. May 26, 2016) (Ex. A). The



**B. Plaintiffs' Allegations**

In March 2016, Plaintiffs Rivera and Weiss, represented by the same counsel, filed suit against Google alleging violations of BIPA. *See* Rivera Dkt. No. 1; Weiss Dkt. No. 1. Pursuant to this Court's order, *see* Rivera Dkt. 30, Weiss Dkt. 30, Google filed a Consolidated Motion to Dismiss both Complaints on May 18. The Court then consolidated the two cases, *see* Rivera Dkt. 36, and each Plaintiff filed a First Amended Complaint on May 27, mooted Google's then-pending Motion to Dismiss, *see* Rivera Dkts. 40, 41.<sup>4</sup>

According to Plaintiffs' First Amended Complaints, Google operates Google Photos, a free "cloud-based" service that lets its users easily upload, organize, and share their photos. *See* FACs ¶¶ 5, 8, 19.<sup>5</sup> Google Photos can organize photos by subject. For example, Google Photos can create virtual albums for "beaches" or "flowers," automatically including all of a user's photos of beaches or flowers. Google also can organize a user's photos based on the images of

---

amendment is "declarative of existing law," and so is intended merely to clarify the language of BIPA. The amendment:

(1) Clarifies the definition of biometric identifiers by adding "physical or digital" before "photographs" ("Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include . . . physical or digital photographs . . .");

(2) Clarifies that "information derived from" photographs is excepted from the definitions of both biometric identifiers and biometric information (" 'Biometric information' and 'biometric identifier' do not include information derived from items or procedures excluded under the definition of biometric identifiers."); and

(3) Defines "scan" to clarify that it means data resulting from an in-person process, not data resulting from a "scan" of a photograph ("Scan" means data resulting from an in-person process whereby a part of the body is traversed by a detector or an electronic beam.")

The Court need not consider the proposed amendment at this time as it has not become law. *See* Bill Status, available at

<http://www.ilga.gov/legislation/BillStatus.asp?DocNum=6074&GAID=13&DocTypeID=HB&LegID=95604&SessionID=88&SpecSess=&Session=&GA=99#actions> (last accessed June 16, 2016).

<sup>4</sup> In its Consolidated Motion to Dismiss, Google noted that Plaintiff Joseph Weiss, who alleges that he is a Google Photos user, necessarily agreed to the choice-of-law provision in Google's Terms of Service and so is precluded from pursuing a claim under BIPA, an Illinois statute. Rivera Dkt. 34, n.1. Google noted that it was not moving to dismiss Weiss' claim on that basis because Weiss may contend that factual issues are implicated, but that it expressly preserves and does not waive its right to more fully assert that defense at a later time. *See* Fed. R. Civ. P. 12(b)(6) (choice of law is not among the defenses that is waived if not asserted in a motion to dismiss). During the status conference on May 24, counsel for Plaintiffs stated that Plaintiffs would not object to Google raising a California choice-of-law argument as to Plaintiff Weiss later in the litigation. Rivera Dkt. 36 (Minute Order). For the same reasons set forth in its Consolidated Motion to Dismiss and discussed at the May 24 status conference, Google expressly preserves and does not waive its right to more fully assert the choice-of-law defense at a later time.

<sup>5</sup> For purposes of this Motion, Google addresses the facts as alleged. Google does not concede that the allegations are accurate. Plaintiffs' description of Google Photos is inaccurate in many respects.

the people in them. For instance, Google Photos can group together all of a user's photos of a particular person. The user can then give any label he or she chooses to that person (e.g., "Dad").

Plaintiffs allege that Google uses facial recognition technology to help users organize their photos of people. *See* FACs ¶¶ 15, 21, 22. According to Plaintiffs, Google uses information "derived from photographs," FACs ¶ 18, to "creat[e]" and store "templates" of the faces in the photos, FACs ¶ 21. Plaintiffs do not allege that Google discloses these templates to anyone. FACs ¶ 22.

Weiss alleges that he has a Google Photos account, to which he uploaded twenty-one photos of himself. Weiss FAC ¶¶ 27, 28. He alleges that Google "extracted" "geometric data" about the image of his face from the photos he uploaded, then used that data and Google's facial recognition technology to create a "face template." *Id.* ¶¶ 5, 29. Weiss does not allege that Google did anything with the template other than use it to help him organize his photos, and to "recognize" his "gender, age, race, and location." *Id.* ¶¶ 30, 31.

Rivera does not have a Google Photos account. She alleges that someone else uploaded approximately eleven photos of her to Google Photos. Rivera FAC ¶¶ 5, 26, 27. Like Weiss, Rivera alleges that Google extracted data from the photos of her face to create a template using facial recognition technology, then used that template to organize photos of her and to recognize her gender, age, race, and location. *Id.* ¶¶ 28-30.

Plaintiffs concede that these so-called templates are "derived from photographs" uploaded to Google Photos. FACs ¶ 18 ("Google's practices of collecting, storing, and using Google Photo users' biometric identifiers and information *derived from photographs* uploaded in Illinois without informed written consent violate" BIPA) (emphasis added). Yet Plaintiffs assert that these so-called templates amount to a "scan" of "face geometry" and so are "biometric identifiers" covered by BIPA. *See* Rivera FAC ¶ 43 (Plaintiff and class members "had their 'biometric identifiers,' including scans of face geometry, . . . obtained by Google from photographs"); Weiss FAC ¶ 44 (same).

In their original Complaints, Plaintiffs sought to represent classes consisting of certain Illinois residents: people who, “while residing in the State of Illinois,” had their “face templates” obtained by Google. Weiss Compl., Weiss Dkt. 1, ¶ 36 (Google Photos users); Rivera Compl., Rivera Dkt. 1, ¶ 35 (Google Photos non-users). In the FACs, Plaintiffs shift their focus to the location where photos are uploaded to Google Photos. Plaintiffs now seek to represent everyone “who had their biometric identifiers, including scans of face geometry, collected, captured, received or otherwise obtained by Google from photographs *uploaded within the state of Illinois*.” Weiss. Compl. ¶ 36 (Google Photos users), Rivera Compl. ¶ 35 (Google Photos non-users) (emphasis added).

Each Plaintiff seeks declaratory and injunctive relief, litigation expenses, attorneys’ fees, and interest, along with statutory damages of \$5,000 for each intentional and reckless, and \$1,000 for each negligent, violation of BIPA. *See* FACs at 15 (Prayers for Relief); 740 ILCS 14/20(1), (2) (BIPA’s statutory damages provisions).

### III. ARGUMENT

#### A. The Text, Structure, and History of BIPA Demonstrate that the Statute Does Not Cover Photographs or Information Derived from Photographs

BIPA regulates “biometric identifiers” and “biometric information.” Even accepting Plaintiffs’ allegations as true, however, this case involves neither: There are no “biometric identifiers” or “biometric information” at issue.

1. A straightforward application of the statute shows why. According to Plaintiffs, Google first obtained *photographs* from Google Photos users, and then *derived information from those photographs* (in the form of so-called “face templates”). FACs ¶¶ 19-23. The General Assembly, however, considered whether BIPA should cover *photographs*, and concluded that it should not; the text of the statute expressly excludes “photographs” from the definition of “biometric identifier.” 740 ILCS 14/10. The General Assembly also considered whether BIPA should cover *information derived from photographs*, and concluded that it should not; the text of the statute expressly excludes “information derived from” photographs from the definition of

“biometric information.” *Id.* Thus, the photographs Google obtained are not “biometric identifiers,” and the information it derived from those photographs is not “biometric information.” Because Google’s alleged conduct involved neither “biometric identifiers” nor “biometric information,” Plaintiffs have failed to state a violation of BIPA.

2. Plaintiffs nevertheless contend that BIPA covers Google’s alleged conduct because *information derived from photographs* can be a “biometric identifier[.]” Rivera FAC ¶ 43; Weiss FAC ¶ 44. According to Plaintiffs, the information here—allegedly consisting of face templates—constitutes a “scan[.] of face geometry.” *Id.* Plaintiffs’ interpretation of the statute, however, cannot be squared with BIPA’s text, structure, or history.

a. Start with the statute’s text. *See S. Illinoisan v. Ill. Dep’t of Pub. Health*, 844 N.E.2d 1, 14 (Ill. 2006) (“In determining legislative intent, our inquiry begins with the plain language of the statute, which is the most reliable indication of the legislature’s objectives in enacting a particular law.”) (citation omitted); *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 615 (7th Cir. 2013) (explaining that this Court’s role is to predict how the Illinois Supreme Court would interpret the statute). BIPA defines “biometric identifier” to mean “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10. These are all things derived from the “biologically unique” features of an actual person. *Id.* 14/5(c). One obtains a “retina . . . scan” by scanning a person’s “retina,” a “fingerprint” by printing a person’s “finger[.]” and so on. *Id.* 14/10. None of these things can be obtained without an actual person present. The same is true of the things that BIPA expressly excludes from the definition of “biometric identifier”—“writing samples, written signatures, photographs, human biological samples,” “X-ray[s],” “MRI[s],” and “PET scan[s],” to name a few. *Id.* All of those things also require the presence of an actual person—to give a sample, to provide a signature, to appear in a photograph, and so on.

The text of the statute thus makes clear that the General Assembly intended the term “biometric identifier” to refer only to things obtained in person, from the biological source itself. It follows that a “scan of . . . face geometry” refers only to a scan of the geometry of a person’s

actual face—that is, it must be derived from the person herself. *See People v. Diggins*, 919 N.E.2d 327, 332 (Ill. 2009) (explaining that under the canon of *noscitur a sociis*, “the meaning of questionable words or phrases in a statute may be ascertained by reference to the meaning of words or phrases associated with it” (internal quotation marks and brackets omitted)). The face templates at issue here do not fit that description. They are derived from photographs, not the persons themselves. They are allegedly “scans” of those photographs, Rivera FAC ¶ 21, not scans of the geometry of a person’s actual face. The face templates therefore do not qualify as “biometric identifiers.”

b. The structure of the statute reinforces this conclusion. The General Assembly provided separate definitions of “biometric identifier” and “biometric information” for a reason. That reason has to do with the source of the content. A “biometric identifier” is something derived from persons themselves. “Biometric information,” by contrast, is one step removed: It is information “*based on* an individual’s biometric identifier.” 740 ILCS 14/10 (emphasis added). Under the statute, therefore, what is derived from a person is a “biometric identifier,” and what is subsequently derived from a biometric identifier is “biometric information.” The statute’s structure thus confirms that a “scan of . . . face geometry” must be derived from the person herself. Plaintiffs’ reading of the statute would collapse this careful structure, rendering the distinction between “biometric identifier” and “biometric information” meaningless. *See Kraft, Inc. v. Edgar*, 561 N.E.2d 656, 661 (Ill. 1990) (“[I]n ascertaining the meaning of a statute, the statute should be read as a whole with all relevant parts considered . . . [and] should be construed so that no word or phrase is rendered superfluous or meaningless.”) (citations omitted).

Plaintiffs’ reading would also make nonsense of another aspect of the statute’s structure: the fact that all of BIPA’s requirements, including the requirements at issue in this case, apply equally to both “biometric identifiers” and “biometric information.” *See, e.g.*, 740 ILCS 14/15(b) (prohibiting a private entity from obtaining a person’s “biometric identifier *or* biometric information” without informed written consent (emphasis added)). Given that the two terms

appear side by side throughout the statute, it would not make sense for the General Assembly to exclude certain things from one category of data, only for those same things to fall within another category. Why would the General Assembly go out of its way to exclude information derived from photographs from “biometric information” if that same information met the definition of “biometric identifier”? The only reasonable inference is that the General Assembly believed that information derived from photographs could not qualify as “biometric identifiers,” and so by excluding such information from “biometric information,” it sought to ensure that such information would not be covered by the statute at all. By treating face templates derived from photographs as “biometric identifiers,” Plaintiffs’ construction of the statute would undermine that legislative intent.

That the General Assembly did not intend information derived from photographs to be “biometric identifiers” finds further support in BIPA’s informed-written-consent provisions. Those provisions require that a private entity get a person’s informed written consent before it obtains her “biometric identifier” or derives any information from it. 740 ILCS 14/15(b). When a scan is conducted in person, there is always an opportunity to get a person’s informed consent; the subject of the scan will be present to provide (or withhold) it. But if “biometric identifier” also included information derived from photographs, that opportunity would, in most cases, not exist. Getting the requisite informed consent would often be practically impossible because one would have to contact every person in the photograph—no matter how long ago the photograph was taken, and no matter whether the individual even knew the person. Because the General Assembly contemplated an opportunity for informed consent when it enacted BIPA, the fact that such an opportunity would often not even exist under Plaintiffs’ reading of the statute demonstrates that their reading is wrong.

c. If there were any remaining ambiguity, the legislative history resolves it. *See Krohe v. City of Bloomington*, 789 N.E.2d 1211, 1214 (Ill. 2003) (“[A] statute’s legislative history and debates are valuable construction aids in interpreting an ambiguous statute.” (internal quotation marks and brackets omitted)).

*First*, when the General Assembly enacted BIPA, it was concerned about data obtained through in-person scans—not information derived from photographs. One cosponsor of the legislation, for example, took to the Senate floor to explain that the bill was “especially important” because Pay By Touch, “the largest fingerprint scan system in Illinois,” had recently filed for bankruptcy, leaving “thousands of customers . . . wondering what will become of their biometric and financial data.” IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249 (May 30, 2008) (Statement of Rep. Kathleen A. Ryg) (Ex. B). The biometric identifiers that Pay By Touch possessed were fingerprints obtained through in-person scans at grocery stores and gas stations. *See* 740 ILCS 14/5(b). And it was the “growing” use of those kinds of “biometrics”—in-person scans “used to access finances or other sensitive information”—that motivated the General Assembly to enact BIPA. *Id.* 14/5(a), (c).

*Second*, there is no indication whatsoever in the legislative record that the General Assembly ever intended to regulate information derived from photographs. That silence speaks volumes, because one must presume that if the General Assembly actually intended to enact a law as sweeping as Plaintiffs suggest, someone would have remarked upon it. After all, under Plaintiffs’ reading, BIPA would prohibit not only Google from operating Google Photos, but also any individual from running common photo-organizing software on a home computer. *See id.* 14/10 (defining “[p]rivate entity” to include “any individual”). What’s more, any individual caught doing so would face thousands of dollars in statutory damages. *See id.* 14/20 (imposing liquidated damages of at least \$1,000 for each statutory violation). If the General Assembly had intended such a result, there would have been at least some discussion of it. The legislature’s “silence in this regard can be likened to the dog that did not bark.” *Chisom v. Roemer*, 501 U.S. 380, 396 n.23 (1991).

*Third*, the General Assembly consciously rejected broader definitions of “biometric identifier.” As originally proposed, the bill defined “biometric identifier” to include “records of hand or facial geometry.” SB 2400, § 10, 95th Gen. Assemb., Reg. Sess. (Ill. Feb. 14, 2008) (Ex. C) (emphasis added). The fact that the General Assembly ultimately opted for the word



“scan” over “records” suggests that it cared about how the content was obtained. Unlike “records,” “scan” suggests something done to the person herself, like an “iris scan” or a “PET scan.” 740 ILCS 14/10. Another version of the bill, which was also not adopted, defined “biometric identifier” to include “facial recognition.” SB 2400, § 10, S. Floor Amend. No. 4, 95th Gen. Assemb., Reg. Sess. (Ill. Apr. 11, 2008) (Ex. D). The General Assembly’s purposeful decision to drop “facial recognition” from the final version further suggests that it did not intend the statute to cover facial recognition technology broadly—only the specific, in-person scans that had prompted it to legislate in the first place. *See Laborer’s Int’l Union of N. Am., Local 1280 v. State Labor Relations Bd.*, 507 N.E.2d 1200, 1204 (Ill. App. Ct. 1987) (“[T]he intent of the state legislature can be derived not only from the language actually adopted, but also from the language which was changed or not adopted.”); *Gulf Oil Corp. v. Copp Paving Co.*, 419 U.S. 186, 200 (1974) (explaining that Congress’s deletion of a provision from a bill “strongly militates against a judgment that [it] intended a result that it expressly declined to enact”).

In short, the text, structure, and history of the statute all point in the same direction: Information derived from photographs cannot be a “biometric identifier.”

3. The decisions of district courts in two other cases should not stand in the way of that conclusion. *See In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747-JD, 2016 WL 2593853 (N.D. Cal. May 5, 2016); *Norberg v. Shutterfly, Inc.*, No. 15-cv-5351, 2015 WL 9914203 (N.D. Ill. Dec. 29, 2015). To begin, this Court is not bound by decisions of other district courts. *See Klein v. Depuy, Inc.*, 476 F. Supp. 2d 1007, 1023 (N.D. Ind. 2007) (“Although federal courts are bound to state court precedents in interpreting state law, there is no authority that requires a district court that is attempting to predict how the highest state court would rule to follow the decision of federal courts sitting in that state.”), *aff’d*, 506 F.3d 553 (7th Cir. 2007); *Midlock v. Apple Vacations W., Inc.*, 406 F.3d 453, 457-58 (7th Cir. 2005) (“[A] district court decision does not have stare decisis effect; it is not a precedent. . . . The fact of such a decision is not a reason for following it.”) (citation omitted).



Moreover, neither of those decisions is persuasive. The decision in *Norberg* contains hardly any reasoning at all, and does not even attempt to explain how BIPA can be read to cover information derived from photographs. The court in *Facebook*, for its part, adopted an interpretation of “photographs” that neither party before it had advanced, construing the term to refer only to “paper prints of photographs, not digitized images.” 2016 WL 2593853, at \*12. That interpretation is contrary to the ordinary meaning of the word “photographs,” which in 2008 was understood (as it is now) to mean *both* digital *and* paper photographs.<sup>6</sup> See *People ex. rel. Stocke*, 80 Ill. App. 3d 109, 115 (5th Dist. 1979) (“Since courts lack legislative powers, we are not permitted to add words to a statute to change its meaning.”) (citation omitted); *Hinkle by Hinkle v. Henderson*, 85 F.3d 298, 304 (7th Cir. 1996) (Under Illinois law, “courts should not insert words into legislative enactments when the statute otherwise presents a cogent and justifiable legislative scheme.”) (citation omitted). That interpretation is unsupported by the legislative history, which contains no indication at all that the General Assembly intended to give such a common term such a restrictive meaning. And if embraced, the *Facebook* court’s interpretation of BIPA would lead to absurd results—among them that just *taking* a digital photograph would constitute a “scan of . . . face geometry,” because such a photograph would no longer fall within the exclusion for “photographs.” Rather than follow these other decisions, this Court should be guided by the text, structure, and history of BIPA and conclude that the statute does not cover information derived from photographs, including digital ones.

\* \* \*

In sum, information derived from photographs—including the face templates at issue in Plaintiffs’ FACs—cannot be “biometric identifiers.” And if face templates are not “biometric identifiers,” then any information derived from them cannot qualify as “biometric information” either. See 740 ILCS 14/10 (“Biometric information does not include information derived from

---

<sup>6</sup> For example, by 2008, digital camera sales far outpaced analog camera sales. See Stephen Dolezalek and Josh Freed, *An American Kodak Moment*, Third Way (Apr. 17, 2014), <http://www.thirdway.org/report/an-american-kodak-moment> (last accessed June 17, 2016).

items or procedures excluded under the definition of biometric identifiers.”). *Contra* Rivera FAC ¶ 30, Weiss FAC ¶ 31. Accordingly, the Court should construe BIPA to exclude information derived from photographs, conclude that Plaintiffs have failed to state a violation of BIPA, and dismiss Plaintiffs’ FACs with prejudice. *See Guinto v. Nestorowicz*, No. 14 C 09940, 2015 WL 3421456, at \*1 (N.D. Ill. May 28, 2015) (granting motion to dismiss with prejudice as to claims that were not cognizable under the circumstances pled by the plaintiff).

**B. Even if BIPA Covers Information Derived from Photographs, the Presumption Against Extraterritoriality Establishes that the FACs Should Be Dismissed**

Even if this Court were to agree with Plaintiffs’ interpretation of “biometric identifier,” Plaintiffs have still failed to allege a violation of BIPA in Illinois. It is a “long-standing rule of construction in Illinois” that “a ‘statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute.’” *Avery v. State Farm Mut. Auto Ins. Co.*, 216 Ill. 2d 100, 184-85 (2005) (quoting *Dur-Ite Co. v. Indus. Comm’n*, 394 Ill. 338, 350 (1946)); *see also Graham v. Gen. U.S. Grant Post No. 2665, V.F.W.*, 43 Ill. 2d 1, 6 (1969) (“when a statute . . . is silent as to extraterritorial effect, there is a presumption that it has none”). There is no indication in the “express provisions of” BIPA that the legislature intended it to apply extraterritorially, so it does not.<sup>7</sup> And Plaintiffs have not alleged that Google “collect[ed]” scans of face geometry or otherwise violated the statute in Illinois. The FACs should therefore be dismissed.

The only link to Illinois alleged in Plaintiffs’ class definitions is that photographs were “uploaded” there. *See* Weiss FAC ¶ 36 (defining class in terms of whether photos were uploaded in Illinois); Rivera FAC ¶ 35 (same). But there is nothing talismanic about the place of upload.

---

<sup>7</sup> Indeed, the express provisions of BIPA suggest the opposite—that it was intended to apply only to biometric-facilitated transactions occurring within the boundaries of Illinois. *See, e.g.*, 740 ILCS 14/5(b) (“Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.”). The legislative history also confirms this. IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249 (May 30, 2008) (Statement of Rep. Kathleen A. Ryg) (Ex. B) (stating that BIPA “will be applicable to private entities doing business in Illinois” and that BIPA is intended to protect “the citizens of Illinois”); *cf. Avery*, 216 Ill. 2d at 184-85 (relying on reference to “the people of [Illinois]” in legislative history to find that the General Assembly did not intend for the statute to apply to fraudulent transactions outside of Illinois).

In *Avery*, the Illinois Supreme Court confronted the question of whether certain consumer transactions had occurred in Illinois so that the plaintiffs could sue under the Illinois Consumer Fraud and Deceptive Business Practices Act, 216 Ill. 2d 185 (2005). That question, the court explained, turned on whether “the circumstances relating to the transaction occur[red] *primarily and substantially* within” Illinois. *Id.* at 186 (emphasis added). A BIPA violation does not “primarily and substantially” occur wherever a photograph happens to be uploaded to Google Photos. The place of upload would, at most, be one “circumstance[.]” informing where the statutory violation “primarily and substantially” occurred. And Plaintiffs cannot elide the multitude of other potentially relevant “circumstances”: where the photo was taken, where the photographer resides, where the subjects of the photo reside, where the Google Photos user signed up for Google Photos, where Google is located, and where Google’s alleged facial recognition analysis takes place. Plaintiffs themselves focused solely on the residency of the photos’ subjects in their original class definitions, demonstrating that even they did not think the place of upload was controlling. *See* Weiss Compl., Weiss Dkt. 1, ¶ 36; Rivera Compl., Rivera Dkt. 1, ¶ 35.

Indeed, to the extent BIPA is read to cover information derived from photographs, the best interpretation of BIPA’s territorial reach is that a violation “primarily and substantially” occurs at the location where that derivation takes place. BIPA makes it unlawful to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier” without written consent. 740 ILCS 14/15(b). The *situs* of a BIPA violation is the place where the unlawful conduct occurs; that is, the place where a biometric identifier is “collect[ed], capture[d], . . . or otherwise obtain[ed].” *Id.* Plaintiffs have not alleged that Google collects, captures, or obtains any biometric information in Illinois. Some Google users upload photographs in Illinois. But under Plaintiffs’ theory, Google violates BIPA not by receiving or storing photographs, but by creating a scan of face geometry *after* the photographs are uploaded. Plaintiffs have not made any allegation that the creation of that scan—the conduct supposedly

prohibited by the statute—occurs in Illinois. Because BIPA does not expressly indicate that it applies to Google’s activities in other jurisdictions, the FACs should be dismissed.

**C. Under Plaintiffs’ Interpretation, BIPA Would Violate the Dormant Commerce Clause**

**1. The Practical Effect of BIPA, on Plaintiffs’ Reading, Is to Regulate Out-Of-State Conduct**

If BIPA is interpreted to apply to information derived from photos, and the presumption against extraterritoriality does not clearly exclude Google Photos from BIPA’s reach, then BIPA would violate the dormant Commerce Clause. The dormant Commerce Clause is a “limitation upon the power of the States.” *Great Atl. & Pac. Tea Co. v. Cottrell*, 424 U.S. 366, 370-71 (1976) (citation omitted). It “protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.” *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 335-37 (1989). In order to determine whether a state statute violates the dormant Commerce Clause in that fashion, the Supreme Court has explained that the “critical inquiry” is “whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.” *Id.* (citation omitted).

Under Plaintiffs’ reading, the “practical effect” of BIPA is just that. Suppose a Google Photos user who lives in Wisconsin takes a photograph of a friend from Iowa and sends it to her friend who lives in Indiana. The Indiana resident receives and uploads the photograph while driving through Illinois, and then Google creates a face template from the photograph on servers in another state. According to Plaintiffs, Illinois can regulate what Google does with the photograph based on an exceedingly tenuous and fortuitous connection—the fact that a user happened to upload it to Google’s cloud servers while passing through Illinois. According to Plaintiffs, regardless of the policies of the three other states at issue in this scenario, Illinois could project its regulatory power into those other states. The Seventh Circuit has “ma[d]e clear” that it “will not hesitate to strike down a state law shown to have extraterritorial scope and an adverse impact on commerce occurring wholly outside the enacting state.” *Nat’l Solid Wastes Mgmt. Ass’n v. Meyer*, 63 F.3d 652, 658-59 (7th Cir. 1995). If BIPA does indeed have the scope

that Plaintiffs think it has, this Court should not hesitate to do the same. *See Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc) (“easily conclud[ing]” that a California statute violated the dormant Commerce Clause because it regulated sales that had “no necessary connection with the state other than the residency of the seller”).

It gets worse. BIPA contains no express geographic limitation on its reach. Under Plaintiffs’ interpretation, it prohibits the use of any facial recognition software without a user’s consent—period. That vast scope would make it impossible for Google to ascertain *ex ante* whether a particular photograph is subject to the constraints of BIPA. *See Am. Civil Liberties Union v. Johnson*, 194 F.3d 1149, 1161 (10th Cir. 1999) (invalidating a New Mexico statute under the Commerce Clause in part because it “contain[ed] no express limitation confining it to communications which occur wholly within its borders”). The uncertainty comes from the fact that Illinois courts may consider various factors to determine whether a photograph is subject to BIPA. And as a consequence, it will often be impossible to ascertain whether a particular photograph satisfies those factors. For instance, there is no way to tell from the face of a photograph who first took it or where the subjects of the photograph reside.

That means Google will not be able to know for sure whether BIPA applies to any given photograph. At the same time, BIPA could subject Google to staggering statutory damages. The upshot is that Google would have no choice but to comply with BIPA nationwide as a precaution.<sup>8</sup> In that way, the “practical effect” of BIPA would be “to control conduct beyond the boundaries of the State.” *Healy*, 491 U.S. at 336; *see also TelTech Sys., Inc. v. McCollum*, No. 08-cv-61664, 2009 WL 10626585, at \*8 (S.D. Fla. July 16, 2009) (holding that a state caller ID statute had the “practical effect” of regulating commerce “wholly outside the state”—and thus violated the dormant Commerce Clause—because it would be “impossible” for parties to determine *ex ante* whether the statute applied to any given call). That is a *per se* violation of the

---

<sup>8</sup> In addition, applying BIPA’s notice and consent requirements to photos makes compliance nearly impossible because of the difficulty of identifying and locating subjects long after the photo was taken. As a result, applying BIPA to photos would result in an effective ban on any technology that arguably made a “scan of . . . face geometry.”

dormant Commerce Clause: A “single State” cannot “enact” a uniform “policy for the entire Nation” or “impose its own policy choice on neighboring States.” *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571 (1996); *Nat’l Solid Wastes Mgmt. Ass’n*, 63 F.3d at 658-59.

A number of courts have recognized the unique constitutional dangers posed by state laws purporting to regulate the Internet. The Second Circuit, for instance, in *American Booksellers Foundation v. Dean*, 342 F.3d 96 (2003), struck down a Vermont law making it illegal to “distribute or give away” pornographic material to minors over the Internet under the dormant Commerce Clause. “Because the internet does not recognize geographic boundaries,” the court observed, “it is difficult, if not impossible, for a state to regulate internet activities without ‘project[ing] its legislation into other States.’” *Id.* at 103 (quoting *Healy*, 491 U.S. at 334). The court held that Vermont’s law had the “practical effect” of regulating out-of-state conduct, because the “the rest of the nation” would be “forced to comply with [Vermont’s] regulation.” *Id.* at 103. Indeed, the court “th[ought] it likely that the internet will soon be seen as falling within the class of subjects that are protected from state regulation because they ‘imperatively demand[] a single uniform rule.’” *Id.* at 104 (quoting *Cooley v. Bd. of Wardens*, 53 U.S. 299, 319 (1851)). This case bears that prophecy out: If Illinois can regulate what is done with photos uploaded, it will necessarily project its regulatory policies into other states. The dormant Commerce Clause protects against just that.

Applying BIPA to cloud photo services raises another dormant Commerce Clause problem: the possibility that other states could attempt to regulate the same photographs in contradictory ways. The “unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation.” *Am. Civil Liberties Union*, 194 F.3d at 1161 (10th Cir. 1999) (quoting *Am. Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 168-83 (S.D.N.Y. 1997)). Other states could enact laws like BIPA that subject Google to inconsistent obligations. Indeed, other states have or have considered their own regulations of biometric data. Even if no other state has passed an inconsistent BIPA-like law yet, that does not mean BIPA is insulated from a Commerce Clause challenge; rather, the

Seventh Circuit has taken “a broader view of inconsistent state policies.” *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 667-68 (7th Cir. 2010). First, other states could pass laws in the same space as BIPA and thus subject Google to overlapping and inconsistent obligations. That possibility means that BIPA is “not one of those matters ‘admitting of diversity of treatment, according to the special requirements of local conditions.’” *Bibb v. Navajo Freight Lines*, 359 U.S. 520 (1959); *see Nat’l Solid Waste Mgmt.*, 63 F.3d at 662 (“If Wisconsin can insist on interstate haulers doing things the Wisconsin way in order to obtain access to the Wisconsin market, other states can insist on similar or different prerequisites to their markets.”). Second, the choice *not* to pass BIPA-like legislation is itself a policy choice, and the existence of BIPA thwarts other states’ ability to make that choice. *See Morley-Murphy Co. v. Zenith Elecs. Corp.*, 142 F.3d 373, 379 (7th Cir. 1998) (“In fact, any state that has chosen a policy more laissez faire than [the regulating state] would have its choices stymied, because the state that has chosen more regulation could always trump its deregulated neighbor.”).

In sum, if BIPA is interpreted to apply to Google Photos, it would have the “practical effect” of regulating conduct occurring entirely outside of Illinois. *Healy*, 491 U.S. at 332. It would also subject Google to inconsistent regulations and usurp the ability of other states to make their own policy choices regarding digital photos. It therefore would run afoul of the dormant Commerce Clause.

## **2. This Court Should Interpret BIPA to Avoid Serious Constitutional Problems**

It is a “cardinal principle” of statutory construction that “where an otherwise acceptable construction of a statute would raise serious constitutional problems, the court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress.” *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988). The Illinois Supreme Court applies the same principle to the interpretation of state statutes. *Wilson v. Dep’t of Revenue*, 169 Ill. 2d 306, 310 (1996) (courts “presume statutes to be constitutional and must construe enactments by the legislature so as to uphold their validity whenever it is reasonably possible to do so.”). As the Seventh Circuit has explained,

“[s]tate courts are no more in the habit of construing state legislation in a way that would violate constitutional limitations than federal courts, and they are well aware that the Supreme Court has held that certain assertions of extraterritorial jurisdiction violate the dormant Commerce Clause.” *Morley-Murphy*, 142 F.3d at 379.

Plaintiffs’ interpretation of BIPA—at the very least—raises serious constitutional questions under the dormant Commerce Clause. Google’s interpretation, by contrast, avoids them entirely: If BIPA is limited to in-person scans, it would be simple to confine its operation to Illinois, and the burden on interstate commerce would be minimized. This Court should thus favor Google’s interpretation and avoid grappling with the significant constitutional issues that would otherwise arise. *See id.* at 379-80 (construing state statute to avoid “significant questions under the Commerce Clause”).

#### IV. CONCLUSION

For all of the foregoing reasons, the Court should grant Google’s motion and dismiss the FACs with prejudice.

Dated: June 17, 2016

GOOGLE INC.,

By: /s/ Susan D. Fahringer  
Susan D. Fahringer

**PERKINS COIE LLP**

Susan D. Fahringer, *admitted pro hac vice*  
SFahringer@perkinscoie.com  
Nicola C. Menaldo, *admitted pro hac vice*  
NMenaldo@perkinscoie.com  
1201 Third Avenue, Suite 4900  
Seattle, WA 98101-3099  
Telephone: 206.359.8000  
Facsimile: 206.359.9000

Sunita Bali, *admitted pro hac vice*  
SBali@perkinscoie.com  
505 Howard Street, Suite 1000  
San Francisco, CA 94105-3204  
Telephone: 415.344.7000  
Facsimile: 415.344.7050



Debra R. Bernard (ARDC No. 6191217)  
DBernard@perkinscoie.com  
131 South Dearborn Street, Suite 1700  
Chicago, Illinois 60603-5559  
Telephone: 312.324.8400  
Facsimile: 312.324.9400